Cloud E-Mail Security | i-FilterG3

Smart and Sophisticated Modern Email Security

Today's email threats move fast, and malicious emails look more and more like benign emails. Growing businesses need predictive email security – defeating today's threats with an eye on tomorrow. Protect sensitive information, and your people, from unwanted and malicious email threats today, and tomorrow, with the latest artificial intelligence.

URL Sandbox
i-Filter analyzes and rewrites URL's the moment a user clicks on it safely and securely blocking malicious links and delayed attacks that frequently bypass most other Email filters. Our Sandbox performs this real-time and instant scan of all hyperlinks to make sure you can rest easy.

Smart Banners
Emails can feel like a dangerous risk with how many external threats there are. Our i-Filter combats these threats with smart banners: Across every email is a banner that lets you know where every email came from and whether it is a trusted sender or not.

Email Encryption
Secure sensitive data and make compliance easy. I-Filter Email push-based encryption automatically scans message bodies and attachments for sensitive data, allowing you to easily establish policies to block or encrypted messages with just a few clicks. Alternatively, give users the option to encrypt emails themselves with our Outlook add-in.

Disaster Recovery and E-Mail Continuity
No email server is safe from crashing and crippling a business, but with our new i-Filter you never lose the ability to read your emails. We create individual email portals for each of your users where they can safely read any incoming emails while the email server is restored.

Stop Ransomware
The most advanced anti-ransomware technology available. I-Filter Email security uses behavioral analysis to stop never-before-seen ransomware and boot record attacks.

Smart
Predictive email security able to block known and unknown threats

Powerful
Stop ransomware, spam, and phishing attacks

Effective
Protect sensitive data with email encryption and data loss prevention

Flexible
Supports O365 and Microsoft Exchange Servers, and Active Directory Synchronization

See the Future

Artificial Intelligence (AI) is built into I-Filter. AI allows i-Filter to be able to detect suspicious payloads containing threats, malware, and unwanted applications, as well as high-level threats embedded in documents, including ransomware. i-Filter detonates these files in series of Virtual machines, simulating a real end user environment where behavior can be monitored, delivering safe documents – not just PDFs.

Block Stealth Attacks

Protecting employees from malicious website links, our advanced URL protection is out smarting attackers who slip phishing URLs past traditional gateways, delaying the upload of malware to websites until after the email is delivered. i-Filter Time-of Click checks website reputation before delivery and at the time you click – blocking stealthy, delayed attacks.

Trust Your Inbox

Phishing imposter defense with i-Filter uses a combination of SPF, DKIM, and DMARC authentication techniques, header anomaly analysis, as well as display name and lookalike domain checks. This allows you to identify and permit legitimate emails while blocking imposters – so you can trust your inbox again.

i-Filter's global threat intelligence network ensures you won't miss the thousands of new spam and malware threats discovered every hour. IP reputation filtering blocks up to 90% of spam at the door, while I-Filter anti-spam and antivirus engines catch the rest.

Protect Sensitive Data

Secure sensitive data and make compliance easy with i-Filter Email push-based encryption and DLP.

Flexible Deployment

i-Filter was born to be flexible. Creating unique security policies for individuals, groups, or the whole domain can be done in minutes – saving you valuable time.

Seamless integration with Outlook or On-Prem Exchange 2003+ allows for easy and quick protection for email services you own. Content Control

Protect sensitive information with discovery of financials, confidential contents, health information, and PII in all emails and attachments.

Search & Destroy

i-Filter uses O365 APIs to directly access O365 mailboxes, allowing i-Filter to identify and automatically remove emails containing malicious links and malware before a user clicks on them – removing the threat automatically.

i-Filter Features

- ✓ Inbound & Outbound Message Scanning
- ✓ Domain / Group / User Policies
- ✓ Admin and User Quarantine
- ✓ Admin Allow / Block Lists
- ✓ 24/7 Emergency Inbox
- ✓ Anti Spam Filters
- ✓ Delay Queue
- ✓ Inbound SPF, DKIM and DMARC
- ✓ Display Name and Lookalike Domain Analysis
- ✓ Anti Virus Filters
- ✓ Time-of-Click URL Protection
- ✓ I-Filter Sandstorm
- ✓ Push-based Email Encryption
- ✓ Enforced TLS encryption
- ✓ Data Loss Prevention
- ✓ Content control policies (keyword and file types)